# USER AUTHENTICATION SYSTEM

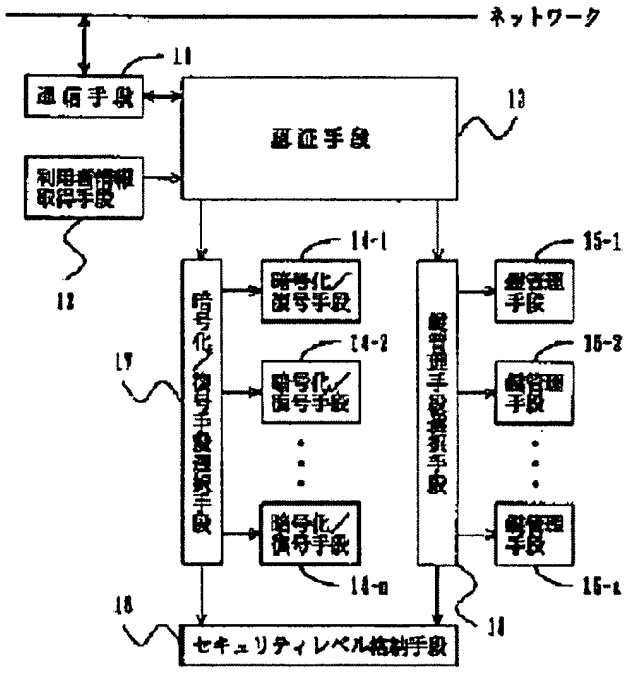
**Patent number:** JP8297638
**Publication date:** 1996-11-12
**Inventor:** SUGIYAMA HIROYUKI; TANABE KATSUHIRO
**Applicant:** NIPPON TELEGR & TELEPH CORP <NTT>
**Classification:**
**- international:** G06F15/00; G06F13/00; G09C1/00; H04L9/00; H04L9/10; H04L9/12
**- european:**
**Application number:** JP19950102521 19950426
**Priority number(s):**



Abstract of **JP8297638**

PURPOSE: To provide the user authentication system which can select any ciphering/deciphering means or a key managing means at different security levels suitable for the request of a user or terminal equipment.

CONSTITUTION: This system is provided with plural ciphering/deciphering means from 14-1 to 14-m corresponding to different security levels, plural key managing means from 15-1 to 15-n corresponding to different security levels, security level storage means 16 for storing the security level for each user or terminal equipment designated in advance, ciphering/deciphering means selecting means 17 for selecting the ciphering/deciphering means from 14-1 to 14-m corresponding to the security levels at the time of ciphering/deciphering processing, and key managing means selecting means 18 for selecting the key managing means from 15-1 to 15-n corresponding to the security levels at the time of key acquisition. Thus, ciphering/deciphering processing or key management suitable for the request of the user or terminal equipment is performed.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平8－297638

(43)公開日　平成８年(1996)11月12日

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | ＦＩ | | | 技術表示箇所 |
|---|---|---|---|---|---|---|---|
| Ｇ０６Ｆ | 15/00 | ３３０ | 9364－5L | Ｇ０６Ｆ | 15/00 | ３３０Ｄ | |
| | 13/00 | ３５７ | 7368－5E | | 13/00 | ３５７Ｚ | |
| Ｇ０９Ｃ | 1/00 | | 7259－5Ｊ | Ｇ０９Ｃ | 1/00 | | |
| Ｈ０４Ｌ | 9/00 | | | Ｇ０６Ｆ | 1/00 | ３７０Ｅ | |
| | 9/10 | | | Ｈ０４Ｌ | 9/00 | Ｚ | |

審査請求　未請求　請求項の数２　ＯＬ　（全 ６ 頁）　最終頁に続く

(21)出願番号　特願平7－102521

(22)出願日　平成７年(1995)４月26日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　杉山　広幸
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　田辺　克弘
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

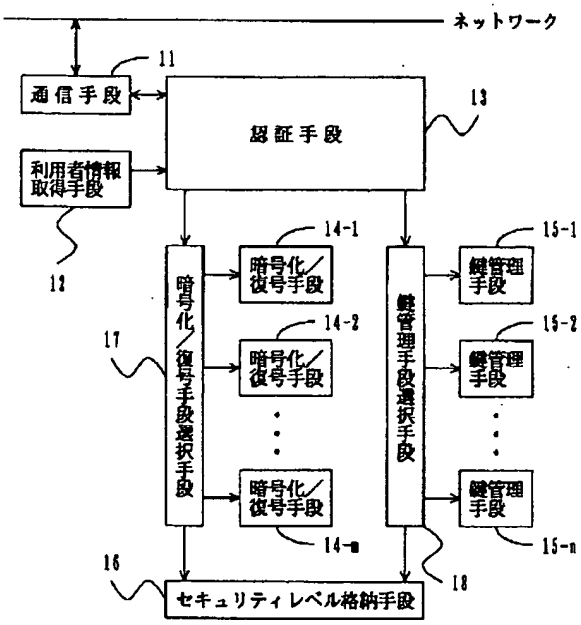
(74)代理人　弁理士　吉田　精孝

(54)【発明の名称】　利用者認証方式

(57)【要約】

【目的】　利用者や端末装置の要求に適したセキュリティレベルの異なる暗号化／復号手段又は鍵管理手段を選択可能な利用者認証方式を提供する。

【構成】　異なるセキュリティレベルに応じた複数の暗号化／復号手段１４－１～１４－ｍと、異なるセキュリティレベルに応じた複数の鍵管理手段１５－１～１５－ｎと、予め指定された利用者や端末装置毎のセキュリティレベルを格納するセキュリティレベル格納手段１６と、暗号化／復号処理時にセキュリティレベルに対応した暗号化／復号手段を選択する暗号化／復号手段選択手段１７と、鍵取得時にセキュリティレベルに対応した鍵管理手段を選択する鍵管理手段選択手段１８とを備えたことにより、利用者や端末装置の要求に適した暗号化／復号処理、鍵管理を行う。



【特許請求の範囲】

【請求項１】　利用者の指示に従ってサービスを要求する端末装置と、サービスを提供するサーバと、これらを接続するネットワークとを備えたクライアントサーバ型分散ネットワークシステムにおける前記利用者がサーバに対してサービスを要求する資格を備えた正規の利用者であることを認証する利用者認証方式において、

異なるセキュリティレベルに応じた暗号化／復号処理をそれぞれ実行する複数の暗号化／復号手段と、

予め指定された利用者や端末装置毎のセキュリティレベルを格納するセキュリティレベル格納手段と、

暗号化／復号処理時に複数の暗号化／復号手段からセキュリティレベル格納手段に格納されたセキュリティレベルに対応した暗号化／復号手段を選択する暗号化／復号手段選択手段とを備えたことを特徴とする利用者認証方式。

【請求項２】　利用者の指示に従ってサービスを要求する端末装置と、サービスを提供するサーバと、これらを接続するネットワークとを備えたクライアントサーバ型分散ネットワークシステムにおける前記利用者がサーバに対してサービスを要求する資格を備えた正規の利用者であることを認証する利用者認証方式において、

異なるセキュリティレベルに応じた鍵管理をそれぞれ実行する複数の鍵管理手段と、

予め指定された利用者や端末装置毎のセキュリティレベルを格納するセキュリティレベル格納手段と、

鍵取得時に複数の鍵管理手段からセキュリティレベル格納手段に格納されたセキュリティレベルに対応した鍵管理手段を選択する鍵管理手段選択手段とを備えたことを特徴とする利用者認証方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、クライアントサーバ型分散ネットワークシステムにおける利用者認証方式に関するものである。

【０００２】

【従来の技術】従来、クライアントサーバ型分散ネットワークシステムにおける認証方式としては、ＭＩＴのAthenaプロジェクトによって開発されたKerberosが広く知られている（Jennifer G.Steiner, Clifford Neuman, Jeffrey I.Schiller, “Kerberos: An Authentication Service for Open Network systems” USENIX Winter Conference, February 9-12, 1988, Dallas, Texas、又はJohn T.Kohl, “The Evolution of Kerberos Authentication Service” Spring, 1991, EurOpen Conference, Tromso, Norway参照）。

【０００３】Kerberosでは、暗号アルゴリズムとしてＤＥＳを採用した、信頼できる第三者に基づく利用者認証機能を提供している。まず、Kerberosにおける利用者認証方式について説明する。

【０００４】図１はクライアントサーバ型分散ネットワークシステムの概要を示すもので、図中、１は利用者の指示に従ってサービスを要求するクライアントコンピュータ（以下、端末装置と称す。）、２はサービスを提供するサーバコンピュータ（以下、単にサーバと称す。）、３はサーバ２に対して端末装置１の利用者が正規の利用者（サーバに対してサービスを要求する資格を備えた利用者）であることを認証する認証サーバコンピュータ（以下、単に認証サーバと称す。）、４は端末装置１、サーバ２及び認証サーバ３を接続するネットワークである。

【０００５】Kerberosにおける利用者認証方式では、端末装置１は利用者から指定されたパスワードよりＤＥＳの鍵である利用者の秘密鍵Ku を生成する手段と、メッセージをＤＥＳアルゴリズムに従って暗号化／復号する手段と、時刻を取得する手段とを有し、サーバ２はサーバ自身であることを示すＤＥＳの鍵であるサーバの秘密鍵Ks を保持する手段と、メッセージをＤＥＳアルゴリズムに従って暗号化／復号する手段と、時刻を取得する手段とを有し、認証サーバ３はＤＥＳの鍵である利用者の秘密鍵Ku 及びサーバ２の秘密鍵Ks の両者を保持する手段と、端末装置１及びサーバ２で共有されるＤＥＳの鍵であるセッション鍵を生成する手段とを有している。

【０００６】以下、Kerberosにおける利用者認証方式をステップ毎に説明するが、この際、Ｅ（Kx , X）はXを鍵Kx で暗号化した値、Ｄ（Kx , X）はXを鍵Kxで復号した値、また、X‖YはXとYとを連結した値をそれぞれ示すものとする。

【０００７】（ステップ１）　利用者の指示に基づいて端末装置１はネットワーク４を経由して認証サーバ３に、サーバ２に対して利用者が正規の利用者であることを証明するために用いるセッション鍵Kusを要求する。

【０００８】（ステップ２）　認証サーバ３は、端末装置１からの要求が該認証サーバ３がその秘密鍵を保持している利用者の指示に基づくものであれば、セッション鍵Kusを生成し、これを該利用者の秘密鍵Ku でＤＥＳアルゴリズムに従って暗号化するとともに、該セッション鍵Kusをサーバ２の秘密鍵Ks でもＤＥＳアルゴリズムに従って暗号化し、端末装置１にネットワーク４を経由してこれらの暗号化されたセッション鍵Ｅ（Ku , Kus）、Ｅ（Ks , Kus）を送る。

【０００９】（ステップ３）　端末装置１は認証サーバ３からネットワーク４を経由して送られてきた、利用者の秘密鍵Ku で暗号化されたセッション鍵Ｅ（Ku , Kus）を、利用者から入力されたパスワードより生成した該利用者の秘密鍵Ku でＤＥＳアルゴリズムに従って復号し、サーバ２とのセッション鍵Kusを得る。

【００１０】（ステップ４）　端末装置１は現在の時刻T1 を取得し、これをセッション鍵KusでＤＥＳアルゴ

リズムに従って暗号化し、認証サーバ３から受け取った前記セッション鍵Ｅ（Ｋｓ，Ｋｕｓ）とともにネットワーク４を経由してサーバ２に送る。

【００１１】（ステップ５）　サーバ２は受け取った前記セッション鍵Ｅ（Ｋｓ，Ｋｕｓ）を、自身の秘密鍵ＫｓでＤＥＳアルゴリズムに従って復号してセッション鍵Ｋｕｓを得る。このセッション鍵Ｋｕｓで端末装置１から送られた、暗号化された時刻Ｅ（Ｋｕｓ，Ｔ１）をＤＥＳアルゴリズムに従って復号し、時刻Ｔ１を得る。

【００１２】そして、現在の時刻Ｔ２を取得し、時刻Ｔ１と時刻Ｔ２とを比較し、Ｔ１＋５分＜Ｔ２であれば、端末装置１にサービスの要求を指示した利用者は正規の利用者であると判断してサービスの提供を開始し、そうでなければ正規の利用者ではないと判断してサービスの提供を拒否する。

【００１３】

【発明が解決しようとする課題】このようにKerberosでは、利用者認証の過程において常にＤＥＳアルゴリズムに従って暗号化／復号を行い、他の異なる暗号アルゴリズムを選択することはできない。しかしながら、実際のシステムにおいてはその形態や提供するサービス等の条件により、個々の利用者や端末装置毎にセキュリティレベル（安全性）の異なる利用者認証方式を採用したい場合がある。

【００１４】例えば、社内の掲示板サービスの場合にはセキュリティレベルが低くてもレスポンスタイムを優先した利用者認証方式を採用したいが、人事システムの場合にはセキュリティレベルが非常に高い利用者認証方式を採用したいという要求がある。この際、掲示板サービスでの利用者認証に用いる暗号アルゴリズムはＦＥＡＬ－８のＣＢＣモードを、人事システムでの利用者認証に用いる暗号アルゴリズムはＦＥＡＬ－３２ＸのＣＢＣモードをというように、要求されるセキュリティレベルに適した暗号アルゴリズムを、同一のシステム内で個々の利用者や端末装置毎に選択できることが望まれる。

【００１５】また同様に、利用者のアイデンティティを示す秘密鍵を管理する手段も、Kerberosでは利用者が記憶したパスワードから自動的に生成する手段のみしか持たず、ハッカーらのパスワードアタックに対しては従来のパスワード入力方式の利用者認証方式と同じ程度の安全性しか提供することができない。

【００１６】しかしながら、現在ではＩＣカード等の極めて安全性の高い装置を利用可能であり、高いセキュリティレベルが要求される場合はコストがかかってもこのような装置を用い、それほどのセキュリティが要求されない場合はKerberosと同様なパスワードから自動的に生成する手段を用いるというように、要求されるセキュリティレベルに適した秘密鍵の管理手段を、同一のシステム内で個々の利用者や端末装置毎に選択できることが望まれる。

【００１７】本発明の目的は、利用者や端末装置の要求に適したセキュリティレベルの異なる暗号化／復号手段を同一のシステム内で選択可能な利用者認証方式を提供することにある。

【００１８】本発明の他の目的は、利用者や端末装置の要求に適したセキュリティレベルの異なる秘密鍵の管理手段を同一のシステム内で選択可能な利用者認証方式を提供することにある。

【００１９】

【課題を解決するための手段】本発明では前記目的を達成するため、請求項１では、利用者の指示に従ってサービスを要求する端末装置と、サービスを提供するサーバと、これらを接続するネットワークとを備えたクライアントサーバ型分散ネットワークシステムにおける前記利用者がサーバに対してサービスを要求する資格を備えた正規の利用者であることを認証する利用者認証方式において、異なるセキュリティレベルに応じた暗号化／復号処理をそれぞれ実行する複数の暗号化／復号手段と、予め指定された利用者や端末装置毎のセキュリティレベルを格納するセキュリティレベル格納手段と、暗号化／復号処理時に複数の暗号化／復号手段からセキュリティレベル格納手段に格納されたセキュリティレベルに対応した暗号化／復号手段を選択する暗号化／復号手段選択手段とを備えた利用者認証方式を提案する。

【００２０】また、請求項２では、利用者の指示に従ってサービスを要求する端末装置と、サービスを提供するサーバと、これらを接続するネットワークとを備えたクライアントサーバ型分散ネットワークシステムにおける前記利用者がサーバに対してサービスを要求する資格を備えた正規の利用者であることを認証する利用者認証方式において、異なるセキュリティレベルに応じた鍵管理をそれぞれ実行する複数の鍵管理手段と、予め指定された利用者や端末装置毎のセキュリティレベルを格納するセキュリティレベル格納手段と、鍵取得時に複数の鍵管理手段からセキュリティレベル格納手段に格納されたセキュリティレベルに対応した鍵管理手段を選択する鍵管理手段選択手段とを備えた利用者認証方式を提案する。

【００２１】

【作用】本発明の請求項１によれば、利用者の認証に伴って該利用者の秘密鍵を用いた暗号／復号化処理を行う際、複数の暗号化／復号手段から暗号化／復号手段選択手段により、セキュリティレベル格納手段に格納された利用者や端末装置毎のセキュリティレベルに対応した暗号化／復号手段を選択することができ、利用者や端末装置毎のセキュリティレベルに応じた利用者の認証を行うことができる。

【００２２】また、請求項２によれば、利用者の認証に伴って該利用者の秘密鍵を取得する際、複数の鍵管理手段から鍵管理手段選択手段により、セキュリティレベル格納手段に格納された利用者や端末装置毎のセキュリテ

ィレベルに対応した鍵管理手段を選択することができ、利用者や端末装置毎のセキュリティレベルに応じた利用者の認証を行うことができる。

【００２３】

【実施例】以下、図面を用いて本発明の実施例を説明するが、ここではISO/IEC 9798-2 “Information technology - Security techniques - Entity authentication mechanisms ; Part 2 ; Entity authentication using symmetric techniques” の “6.2 Five pass authentication” に示される慣用鍵暗号アルゴリズムに基づく信頼できる第三者を用いた５パス認証方式に本発明を適応した例を示す。

【００２４】本実施例におけるクライアントサーバ型分散ネットワークシステムの概要は図１に示したものと同様である。

【００２５】図２は本実施例における端末装置を示すもので、図中、１１は通信手段、１２は利用者情報取得手段、１３は認証手段、１４－１，１４－２，……１４－mは暗号化／復号手段、１５－１，１５－２，……１５－nは鍵管理手段、１６はセキュリティレベル格納手段、１７は暗号化／復号手段選択手段、１８は鍵管理手段選択手段である。

【００２６】通信手段１１はネットワーク４に接続され、サーバ２及び認証サーバ３と通信を行う。利用者情報取得手段１２は利用者から利用者識別子を取得する。認証手段１３は前記ISO 9798-2に基づく認証方式を実施する。

【００２７】暗号化／復号手段１４－１～１４－mは異なるセキュリティレベルに応じた暗号化／復号処理をそれぞれ実行するもので、ＦＥＡＬ、ＤＥＳ等の各種の異なるアルゴリズムや、ＥＢＣモード、ＣＢＣモード、ＣＦＢモード、ＯＦＢモード等の暗号アルゴリズムの各種の異なる利用モードを備えている。鍵管理手段１５－１～１５－nは異なるセキュリティレベルに応じた秘密鍵の管理を実行するもので、ＩＣカードやＰＣＭＣＩＡカード、ＲＯＭ等の各種の異なるハードウェアを備えている。

【００２８】セキュリティレベル格納手段１６は予め指定された利用者や端末装置毎のセキュリティレベルを格納する。暗号化／復号手段選択手段１７は暗号化／復号手段１４－１～１４－mのうち、セキュリティレベル格納手段１６に格納されているセキュリティレベルに対応したものを認証手段１３からの要求に基づいて選択する。鍵管理手段選択手段１８は鍵管理手段１５－１～１５－nのうち、セキュリティレベル格納手段１６に格納されているセキュリティレベルに対応したものを認証手段１３からの要求に基づいて選択する。

【００２９】図３は本実施例における端末装置１、サーバ２及び認証サーバ３間でやりとりされるメッセージのシーケンスを示すもので、以下、本実施例における認証動作を説明する。

【００３０】まず、端末装置１は、利用者情報取得手段１２を用いて利用者の識別子ＩＤuを取得する。次に、認証手段１３にその利用者識別子ＩＤu を渡し、認証手段１３はその利用者識別子ＩＤu と生成した乱数Ru からメッセージＭ１を作成し、通信手段１１を介してサーバ２に送る。

【００３１】サーバ２は、サーバの識別子ＩＤs と生成した乱数Rs1とメッセージＭ１中のＩＤu 、Ru からメッセージＭ２を作成し、認証サーバ３に送る。

【００３２】認証サーバ３は、利用者識別子ＩＤu 、サーバ識別子ＩＤs から各々の登録されている秘密鍵Ku 、Ks を取得し、さらに端末装置１とサーバ２で共有するセッション鍵Ksuを生成する。次に、このセッション鍵Ksuと端末装置１から送られてきた乱数Ru 、サーバ２から送られてきた乱数Rs1を各々連結し、さらに利用者の秘密鍵Ku 、サーバ２の秘密鍵Ks でそれらを各々暗号化し、メッセージＭ３、即ちＥ（Ku , Ru ‖ Ksu）、Ｅ（Ks , Rs1‖Ksu）を作成し、サーバ２へ送り返す。

【００３３】サーバ２は、メッセージＭ３の一部であるＥ（Ks , Rs1‖Ksu）を、サーバ２の秘密鍵Ks で復号し、乱数Rs1、セッション鍵Kusを取得する。ここで取得した乱数とメッセージＭ２で送った乱数とを照合し、一致すればメッセージＭ３を正しい認証サーバ３からの応答であると判断し、以後の動作を継続する。

【００３４】次に、サーバ２は、新たな乱数Rs2を生成し、端末装置１からメッセージＭ１で送られてきた乱数Ru と連結し、セッション鍵Kusで暗号化し、メッセージＭ３の残りの部分とともにメッセージＭ４、即ちＥ（Ku , Ru ‖ Ksu）、Ｅ（Ksu, Ru ‖ Rs2）を作成し、端末装置１へ送る。

【００３５】端末装置１は、メッセージＭ４を通信手段１１で受け取り、認証手段１３に渡す。認証手段１３はメッセージＭ４の認証サーバ３から送られてきた部分Ｅ（Ku , Ru ‖ Ksu）を復号するために、まず、鍵管理手段選択手段１８に利用者の秘密鍵Ku の取得を要求する。

【００３６】鍵管理手段選択手段１８はセキュリティレベル格納手段１６にセキュリティレベルを問い合わせる。セキュリティレベル格納手段１６は、自身が格納しているセキュリティレベルを鍵管理手段選択手段１８に伝える。鍵管理手段選択手段１８はセキュリティレベル格納手段１６から知らされたセキュリティレベルに従って、鍵管理手段１５－１～１５－nの中から適切な鍵管理手段を選択し、その鍵管理手段を用いて利用者の秘密鍵Ku を取得し、認証手段１３に渡す。

【００３７】次に、認証手段１３は暗号化／復号手段選択手段１７に、鍵管理手段選択手段１８から得た利用者の秘密鍵Ku によるＥ（Ku , Ru ‖ Ksu）の復号を要

求する。暗号化／復号手段選択手段１７はセキュリティレベル格納手段１６にセキュリティレベルを問い合わせる。セキュリティレベル格納手段１６は、自身が格納しているセキュリティレベルを暗号化／復号手段選択手段１７に伝える。

【００３８】暗号化／復号手段選択手段１７は、セキュリティレベル格納手段１６から知らされたセキュリティレベルに従って、暗号化／復号手段１４－１～１４－ｍの中から適切な暗号化／復号手段を選択し、その暗号化／復号手段を用いてＥ（Ku，Ru ‖Ksu）の復号を行い、乱数Ru 、セッション鍵Kusを取得し、認証手段１３に渡す。

【００３９】認証手段１３は、暗号化／復号手段選択手段１７から取得した乱数とメッセージＭ１で送った乱数とを照合し、一致すればメッセージＭ４を正しい認証サーバからの応答であると判断し、以後の動作を継続する。

【００４０】次に、得られたセッション鍵KusでメッセージＭ４の認証サーバ３から送られてきた部分Ｅ（Ksu，Ru ‖Rs2）の復号を暗号化／復号手段選択手段１７に要求する。暗号化／復号手段選択手段１７はセキュリティレベル格納手段１６にセキュリティレベルを問い合わせる。セキュリティレベル格納手段１６は、自身が格納しているセキュリティレベルを暗号化／復号手段選択手段１７に伝える。

【００４１】暗号化／復号手段選択手段１７は、セキュリティレベル格納手段１６から知らされたセキュリティレベルに従って、暗号化／復号手段１４－１～１４－ｍの中から適切な暗号化／復号手段を選択し、その暗号化／復号手段を用いてＥ（Ksu，Ru ‖Rs2）の復号を行い、乱数Ru 、乱数Rs2を取得し、認証手段１３に渡す。

【００４２】認証手段１３は、暗号化／復号手段選択手段１７から取得した乱数Ru と、メッセージＭ１で送った乱数とを照合し、一致すればメッセージＭ４を正しいサーバ２からの応答であると判断し、以後の動作を継続する。

【００４３】次に、認証手段１３は、得られたセッション鍵Kusでサーバ２から送られてきた乱数Rs2と乱数Ru の暗号化を、暗号化／復号手段選択手段１７に要求する。暗号化／復号手段選択手段１７はセキュリティレベル格納手段１６にセキュリティレベルを問い合せる。セキュリティレベル格納手段１６は、自身が格納しているセキュリティレベルを暗号化／復号手段選択手段１７に伝える。

【００４４】暗号化／復号手段選択手段１７は、セキュリティレベル格納手段１６から知らされたセキュリティレベルに従って、暗号化／復号手段１４－１～１４－ｍの中から適切な暗号化／復号手段を選択し、その暗号化／復号手段を用いて乱数Rs2と乱数Ru の暗号化を行い、認証手段１３に渡す。

【００４５】認証手段１３は得られたＥ（Ksu，Rs2‖Ru ）をメッセージＭ５として、通信手段１１を介してサーバ２に送る。

【００４６】サーバ２は、送られてきたメッセージＭ５をセッション鍵Kusで復号し、乱数Ru 、Rs2を取得する。取得した乱数Rs2とメッセージＭ４で送った乱数とを照合し、一致すればメッセージＭ５を正しい端末装置１からの応答であると判断する。

【００４７】

【発明の効果】以上説明したように、請求項１の発明によれば、利用者の認証に伴って該利用者の秘密鍵を用いた暗号／復号化処理を行う際、複数の暗号化／復号手段から暗号化／復号手段選択手段により、セキュリティレベル格納手段に格納された利用者や端末装置毎のセキュリティレベルに対応した暗号化／復号手段を選択することができ、利用者や端末装置毎のセキュリティレベルに応じた利用者の認証を行うことができ、コスト、端末装置の性能や設置場所等の利用者や端末装置側の条件に応じた最適のセキュリティを実現することができる。

【００４８】また、請求項２の発明によれば、利用者の認証に伴って該利用者の秘密鍵を取得する際、複数の鍵管理手段から鍵管理手段選択手段により、セキュリティレベル格納手段に格納された利用者や端末装置毎のセキュリティレベルに対応した鍵管理手段を選択することができ、利用者や端末装置毎のセキュリティレベルに応じた利用者の認証を行うことができ、コスト、端末装置の性能や設置場所、ＩＣカード装置の有無等の利用者や端末装置側の条件に応じた最適のセキュリティを実現することができる。

【図面の簡単な説明】

【図１】クライアントサーバ型分散ネットワークシステムの概要を示す構成図

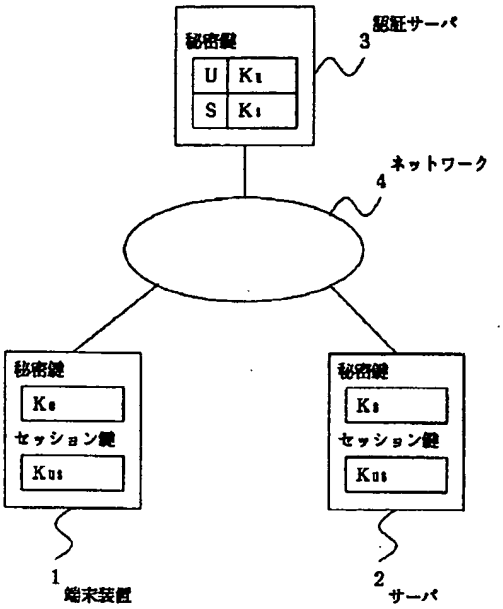
【図２】本発明方式を適用した端末装置の一実施例を示す構成図

【図３】端末装置、サーバ及び認証サーバ間でやりとりされるメッセージのシーケンスを示す図

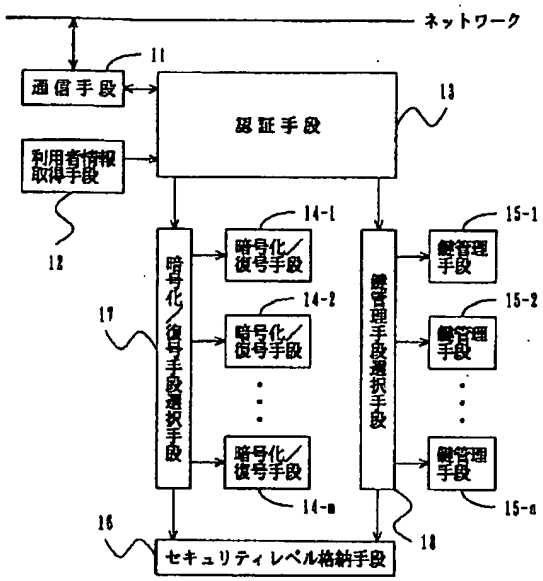
【符号の説明】

１…端末装置、２…サーバ、３…認証サーバ、４…ネットワーク、１１…通信手段、１２…利用者情報取得手段、１３…認証手段、１４－１～１４－ｍ…暗号化／復号手段、１５－１～１５－ｎ…鍵管理手段、１６…セキュリティレベル格納手段、１７…暗号化／復号手段選択手段、１８…鍵管理手段選択手段。

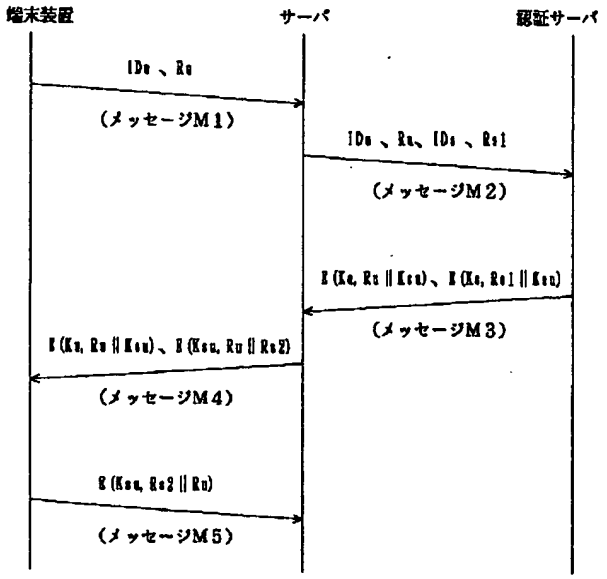
【図１】




【図２】




【図３】




---

フロントページの続き

| (51) Int. Cl.[6] | 識別記号 | 庁内整理番号 | F I | 技術表示箇所 |
|---|---|---|---|---|
| H04L 9/12 | | | | |
| // G06F 1/00 | | 370 | | |